Texas Cybersecurity Weekly

Collected news & information for Texas' cybersecurity community

TLP:WHITE

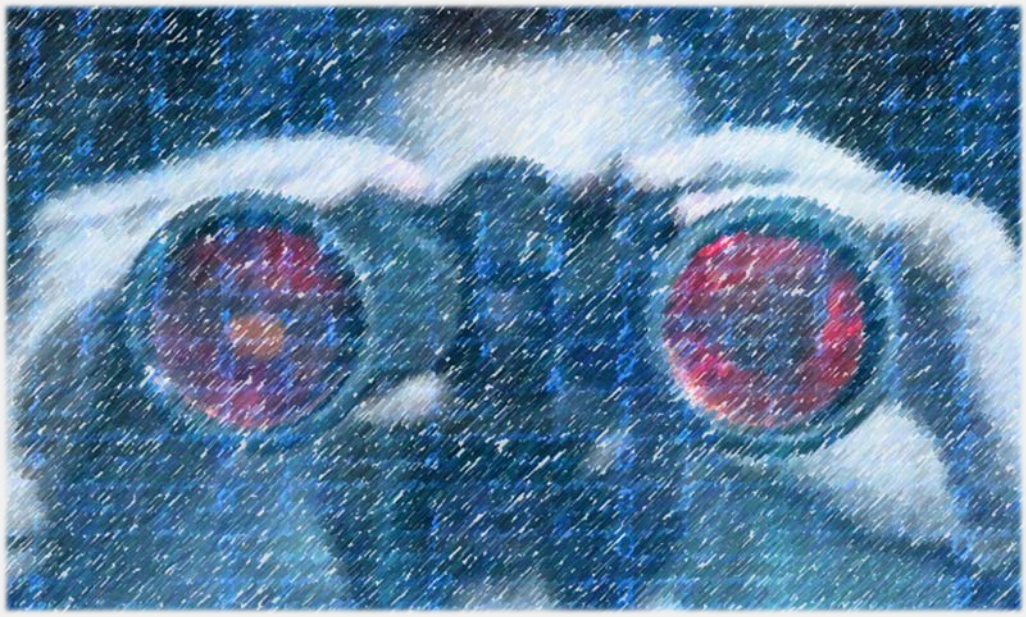
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

Assistance/Feedback/Questions?

Email the Office of the CISO at
DIRSecurity@dir.texas.gov

The periodical aggregates information about cybersecurity and information technology to promote shared awareness, cyber hygiene, and information sharing amongst government, the private sector, and all Texans.

Advisories



Russian Malicious Cyber Activity

April 16, 2018 – Department of Homeland Security

The Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and the United Kingdom's (UK) National Cyber Security Centre (NCSC) released a joint Technical Alert (TA) about malicious cyber activity carried out by the Russian Government. The U.S. Government refers to malicious cyber activity by the Russian government as GRIZZLY STEPPE.
NCCIC encourages users and administrators to review the GRIZZLY STEPPE - Russian Malicious Cyber Activity page, which links to TA18-106A – Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices, for more information.

Ransomware – Cryptomix – Mole66 Variant

Since March 2016, when CryptoMix was discovered, there have been over two dozen variants of the ransomware. On March 29, 2018, the latest variant known as Mole66 was discovered by security researchers. Like previous versions of CryptoMix, Mole66 is a barebones ransomware without a GUI or desktop background change. Victims are instead presented with a text file and web page containing a basic ransom note. Historically, ransom demands for CryptoMix variants have been significant; reportedly upwards of $5,000 to decrypt one computer. There is currently no free way to decrypt this variant of CryptoMix.
It is currently unknown how Mole66 is being spread, however, previous versions of Cryptomix were spread via email with malicious attachments, and through vulnerabilities Remote Desktop Protocol (RDP). Read More:
https://www.bleepingcomputer.com/news/security/mole66-cryptomix-ransomware-variant-released/

Ransomware – AVCrypt

A new ransomware named AVCrypt was discovered by security researches on March 22, 2018. AVCrypt is unique because it is the first ransomware discovered that tries to uninstall existing security software before it encrypts a victim's computer. In addition, AVCrypt removes numerous services, including Windows Update, and provides no contact information in the ransom note. The fact that AVCrypt drops a blank ransom note with no contact information has researchers debating whether the ransomware is still in development. Regardless, AVCrypt is noteworthy and quite destructive to infected computers. Once on a victim's computer, AVCrypt extracts an embedded TOR client and connects to its command & control server (see TOR address in IOC section of this report). It will eventually transmit the encryption key, time zone, and Windows version of the victim's computer to this server. Then AVCrypt attempts to remove installed security software.

Read more: https://www.bleepingcomputer.com/news/security/the-avcrypt-ransomware-tries-to-uninstall-your-av-software/

Ransomware - Matrix

Two new variants of Matrix Ransomware were recently discovered by security researchers. Both variants are being distributed to victims by attackers brute forcing the passwords of Remote Desktop Services connected directly to the Internet. Once the attackers gain access to a computer, they upload the installer and execute it. There are no known ways to decrypt either variant of Matrix Ransomware for free. Security researchers recommend that no computers running Remote Desktop Services be connected directly to the internet. Instead, they should be placed behind VPNs so they are only accessible to authorized users on the network.

Currently, two different variants of Matrix Ransomware are being distributed. Both variants are installed over hacked Remote Desktop Services, encrypt unmapped network shares, display status windows while encrypting, clear shadow volume copies, and encrypt the filenames. However, there are slight differences between the variants, with one being a bit more advanced.

Read More: https://www.bleepingcomputer.com/news/security/new-matrix-ransomware-variants-installed-via-hacked-remote-desktop-services/

Ransomware – GandCrab

On April 10, 2018, Malware-Traffic-Analysis.net reported updated IOCs for a version of GandCrab that is being distributed via malspam. See updated IOCs below.

GandCrab is a Russian ransomware as a service that was first observed on January 26, 2018 during a three-day campaign. The ransomware is introduced to the victim's computer via spam or malvertising. Once a system is infected, all files are encrypted, and a ransom payment is demanded to be paid in the lesser-known Dash cryptocurrency. This is the first ransomware to demand payment in this currency. Unfortunately, to date there is no way to decrypt files encrypted by GandCrab for free. At this time, it is unclear whether GandCrab attempts to spread laterally

See Updated IOCs: https://www.malware-traffic-analysis.net/2018/04/10/index.html

Cryptominer – Rarog

Rarog is a cryptomining trojan – first observed for sale on the Dark Web in June 2017 – that has been used by countless criminals to infect nearly 200,000 victims spread across the globe. To date, more than 2,500 unique Rarog samples, and 161 Command and Control (C2) servers have been discovered. Most

recently, Rarog was used in attacks against ecommerce websites running the popular open-source Magento platform. The tool is appealing to hackers because it is affordable, easily configurable, and supports multiple cryptocurrencies. Security researchers believe we will continue to see increasing use of Rarog and other cryptocurrency miners by hackers.
Read more: https://threatpost.com/rarog-trojan-easy-entry-for-new-cryptomining-crooks-report-warns/130995/

Vulnerability Alerts

Bulletin (SB18-106)
Vulnerability Summary for the Week of April 9, 2018

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

High - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0

Medium - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9

Low - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch

information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis
https://www.us-cert.gov/ncas/bulletins/SB18-106

Multiple Vulnerabilities in Juniper Products Could Allow for Remote Code Execution

MS-ISAC Advisory Number – 2018-041

Date Issued: 04/13/2018

Multiple vulnerabilities have been discovered in Juniper products, the most severe of which could allow for remote code execution. Successful exploitation of the most severe of these vulnerabilities could result in the attacker gaining control of the affected system. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-juniper-products-could-allow-for-remote-code-execution_2018-041/

A Vulnerability in Drupal Could Allow for Remote Code Execution

MS-ISAC Advisory Number – 2018-033

Date Issued: 03/28/2018

A vulnerability has been discovered in the Drupal core module, which could allow for remote code execution. Drupal is an open source content management system (CMS) written in PHP. Successful exploitation of this vulnerability could allow for remote code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.
https://www.cisecurity.org/advisory/a-vulnerability-in-drupal-could-allow-for-remote-code-execution_2018-033/

Oracle Quarterly Critical Patches Issued April 17, 2018

MS-ISAC Advisory Number – 2018-042

Date Issued: 04/17/2018

Multiple vulnerabilities have been discovered in Oracle products, which could allow for remote code execution.
https://www.cisecurity.org/advisory/oracle-quarterly-critical-patches-issued-april-17-2018_2018-042/

Annual Industry Reports

Darktrace Global Threat Report 2017

Cybersecurity has risen to the consciousness of not only nation states, but of business leaders and company boards. High-profile hacks against corporations, many of which are household names, only serve to remind us that no one is invulnerable to cyber-attacks.
https://www.darktrace.com/resources/wp-global-threat-report-2017.pdf

Breach Events

Shutterfly Reacts to Data Breach
April 5, 2018 – Enterprise Time

Web-based printing company Shutterfly has warned employees and former employees that their data may have been compromised. The breach was discovered on March 20 although the company is not saying how.
The company disclosed the breach in a filing with the Office of the Attorney General for California. It says that: *"On March 20, 2018, we learned that a Shutterfly employee's credentials were used without authorization to access our Workday test environment on January 11, 2018. We do not yet know if unauthorized access occurred at other times.*
https://www.enterprisetimes.co.uk/2018/04/05/shutterfly-reacts-to-data-breach/

Ikea app Task Rabbit reveals security breach
April 17, 2018 – BBC News

Ikea's odd jobs marketplace TaskRabbit is investigating a "cybersecurity incident", the company has announced. The app and website let people find freelance workers to complete household tasks such as cleaning, gardening or assembling flat-pack furniture. TaskRabbit has not revealed the nature of the incident, but said it was working with law enforcement and a cybersecurity firm to investigate.
http://www.bbc.com/news/technology-43796596

News and Commentaries

WannaCry Ransomware Sinkhole Data Now Available to Organizations
10 April 2018 – Bleeping Computer

The cybersecurity firm running the main WannaCry sinkhole, announced today plans to allow organizations access to some of the WannaCry sinkhole data. The security firm cites recurring WannaCry ransomware infections that are still taking place…even eleven months after the first WannaCry outbreak

in May 2017. For example, Boeing, Connecticut state agencies, Honda, and Victoria state police suffered WannaCry infections long after the WannaCry killswitch domain was registered, effectively stopping the global outbreak May 2017. The reason that WannaCry continues to make problems is that many organizations have not patched Windows systems by applying the MS17-010 security update that mitigates the vulnerability used by EternalBlue, the exploit at the heart of WannaCry's self-spreading module. Read more here: https://www.bleepingcomputer.com/news/security/wannacry-ransomware-sinkhole-data-now-available-to-organizations/

Avoiding the Ransomware Mistakes that Crippled Atlanta
April 11, 2018 – Dark Reading

Last month, five of Atlanta's 13 government offices were "hijacked," as the city's mayor put it, by ransomware that disrupted far-reaching facets of the city's digital infrastructure. From the courts to the police department to public works, government activity was essentially frozen as the hackers gave the city a week to pay the ransom – roughly $50,000 worth of bitcoin – or have critical data and processes deleted permanently. While the event was eye-catching for several reasons, it's hardly an isolated incident. From Dallas to Denver, hackers leveraging ransomware not unlike the program that hit Atlanta have been able to "hijack" municipal networks largely because these entities were poorly protected. But what made Atlanta such an easy target – even for a relatively common form of ransomware – was its incredibly outdated use of technology in the broader sense. Read more here: https://www.darkreading.com/partner-perspectives/avoiding-the-ransomware-mistakes-that-crippledatlanta/a/d-id/1331518

Hackers Have Started Exploiting Drupal RCE Exploit Released Yesterday
April 13, 2018 – The Hacker News

Hackers have started exploiting a recently disclosed critical vulnerability in Drupal shortly after the public release of working exploit code.
Two weeks ago, Drupal security team discovered a highly critical remote code execution vulnerability, dubbed Drupalgeddon2, in its content management system software that could allow attackers to completely take over vulnerable websites.
https://thehackernews.com/2018/04/drupal-rce-exploit-code.html

Arizona Updates Data Breach Notice Law with Capped Penalties
April 13, 2018 – Bloomberg BNA
Companies in Arizona hit with a data breach will now face up to $500,000 in civil fines from the state attorney general if they don't notify affected consumers within 45 days, under a new law signed by Governor Doug Ducey (R).
https://www.bna.com/arizona-updates-data-n57982091120/

Workforce Development and Events

REGISTRATION IS NOW OPEN for the 18th annual Information Security Forum, to be held May 23-24, 2018 at the Palmer Events Center in Austin, Texas, and is hosted by the Texas Department of Information Resources (DIR) and managed by the Office of the Chief Information Security Officer (OCISO).

http://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=140

The Texas-Israel Chamber of Commerce will hold the watershed Texas-Israel Cyber Security Conference on Thursday, May 31, 2018 at the Martha Proctor Mack Ballroom, on the SMU Campus. For more information on the conference please visit *www.texasisrael.org*.
Registration can be found at http://blog.smu.edu/events/texas-israel-cyber-security/

Government Technology's passion is helping spread best practices and spurring innovation in the public sector. The Texas Digital Government Summit is designed to do just that. The summit has an advisory board that gathers public and private sector leaders to create an agenda designed to make that passion relevant and actionable to the state and local government organizations attending the summit.
http://www.govtech.com/events/Texas-Digital-Government-Summit.html

Texas Government Data Forum 2018

Thursday, June 21, 2018 | 8:00 am - 4:30 pm | Austin, TX

Annual conference hosted by the Texas Department of Information Resources. Any government/public sector employees may attend.

http://dir.texas.gov/View-About-DIR/Calendar-Detail.aspx?id=456&month=6&year=2018&type=list#detail